Enhancing System Reliability using Abstraction and Efficient Logical Computation(Abstract_要旨)

AUTHOR(S):

Kutsuna, Takuro

CITATION:

Kutsuna, Takuro. Enhancing System Reliability using Abstraction and Efficient Logical Computation. 京都大学, 2015, 博士(情報学)

ISSUE DATE:

2015-09-24

URL:

https://doi.org/10.14989/doctor.k19335

（ 続紙 １ ）

京都大学	博士（　　情報　　学）	氏名	沓　名　拓　郎
論文題目	Enhancing System Reliability using Abstraction and Efficient Logical Computation （抽象化技術と高速な論理演算を利用したシステムの高信頼化）		

（論文内容の要旨）

本論文は，自動車に搭載されるシステム，すなわち車載システムの信頼性を向上することを目的としている．車載システムに組み込まれるソフトウェアは年々巨大化する傾向にあり，その信頼性を向上させることは自動車の安全性を確保するために不可欠である．本論文はこのような状況を念頭に置きつつ，４つの領域において，システムの機能あるいは計測データを抽象化して論理式で表現し，高速な論理演算を利用することによりシステムの信頼性を向上させる手法を提案している．

第１章は序章であり，車載システムに用いられるソフトウェアの高信頼化の必要性と，高信頼化の適用領域を挙げた後，本論文の概要を示している．

第２章では，車載システムに組み込まれる制御ソフトウェアをテストするための入出力パターンを自動生成する手法を提案している．有界モデル検査に基づいて記述された論理式の充足可能性を判定することによりテスト・パターンを生成する際には，三角関数や対数関数，あるいは表形式で表現された関数などがソフトウェア中に用いられると，テスト・パターンの生成の計算時間が増大する．提案手法では，入出力が実数値である関数を，入出力が区間の集合である関数に抽象化して論理式で表現するという方法を採用し，具体的な抽象化については機械学習を利用して求める．さらに検証用のソフトウェアを用いて実験することにより，抽象化を用いない方法と比較して，提案手法が高速にテスト・パターンを生成可能であることを確認している．

第３章では，システムから計測された多次元の実数値データについて，訓練データの集合を用いて新たなデータが異常であるかどうかを検知するために，二分決定図(BDD)を用いた１クラス識別器を提案している．１クラス識別器は各訓練データの集合を用いてパラメータを調整することが困難であるという問題がある．提案手法では，[0,2^m]区間内の実数に対する２進符号化を利用して訓練データを論理式で表現した上で，BDDという形で訓練データの集合を表現することにより，異常なデータを検出する．２進符号化はちょうど前章における抽象化に相当する．さらに，提案手法が連続値と離散値の混在データに適用可能であることも示している．また，識別器に学習させる際のパラメータは最小記述長(MDL)原理により決定する方法を提案した上で，人工データと実データを用いて従来手法以上の性能を持つことを確認している．

第４章では，前章の内容を発展させ，二分決定図を用いて多次元の実数データの集合の中から外れデータを検出する手法を提案している．前章と同様に[0,2^m]区間内の実数を２進符号で表現した上で，多次元の実数値データにおける外れデータを，LOO(leave-one-out)濃度が予め与えられた閾値より小さいもの，と定義している．データ集合から構成されたBDDを構成する各節点が[0,2^m]区間内の領域を表現していることに着目し，このBDDを用いて各データのLOO濃度を高速に計算するアルゴリズムを与えている．この手法についても連続値と離散値の混在データに適用可能である．レポジトリで公開されているデータを用いて，提案手法が従来手法と比較して，高精度かつ高速に外れデータを検出することを確認している．

第５章では，車載システムの故障個所を特定する手法を提案している．現在の車載システムにおいては複数の電子制御ユニット(ECU)がネットワーク経由で協調制御を行うため，１つのECUで発生したエラー信号が他のEUCに伝播しうる．提案手法ではモデルベース診断の枠組みに基づいて，ECUで構成されるネットワークの機能を抽象化して論理式で記述した上で，最大充足可能性問題を解くことで伝播したエラー信号の根源箇所を特定する．その際に伝播が複雑なループをなす状況が問題となるが，ルー

プ上で成立する機能的な関係を表す論理式を追加することにより，エラー信号の根源を特定している．当該分野で用いられる検証用システム用いて提案手法の有効性を確認している．

第６章では，本論文で与えた結果を概観し，結論としている．

注)論文内容の要旨と論文審査の結果の要旨は１頁を３８字×３６行で作成し、合わせて、３,０００字を標準とすること。
論文内容の要旨を英語で記入する場合は、４００～１,１００wordsで作成し
審査結果の要旨は日本語５００～２,０００字程度で作成すること。

（続紙 ２ ）

（論文審査の結果の要旨）

本論文は，多数のシステムが搭載された自動車の安全性を確保するために，車載システムの信頼性を向上させるための手法を構築することを目的としている．現代の車載システムは巨大なソフトウェアが組み込まれており，同一の車内で複数のシステムがネットワークで繋がって構成されている．このような複雑な車載システムの信頼性を向上させるために，本論文は，システムの機能あるいは計測データを抽象化して論理式で表現し，高速な論理演算を適用するという方針に基づいて，システムの信頼性を向上させる手法を提案している．主要な結果は以下の４つである．

１．車載システムに組み込まれる制御ソフトウェアをテストするための入力パターンを自動生成することを目的とし，入出力が実数値であるような関数を入出力が区間の集合である関数に抽象化した上で，有界モデル検査に基づいて論理式で表現し，その充足可能性を判定することによりテスト・パターンを生成する手法を構成した．さらに関数の抽象化を求めるために機械学習を利用すること可能であることを示している．結果として，数学的な関数あるいは表形式で実装された関数を含むソフトウェアに対してテスト・パターンを高速に構成することが可能となった．

２．システムから計測された多次元の実数値データに対して，新たに計測されたデータが異常であるかどうかを検知することを目的とし，[0,2^m]区間内の実数に対する抽象化の一種とみなせる２進符号化に基づいて，訓練データの集合をBDDによって表現することにより１クラス識別器を構成した．この識別器は連続値と離散値の混在データにも適用可能である．さらに連続値と離散値の混在データに適用可能であることを示し，また識別器に学習させる際にはパラメータを最小記述長(MDL)原理により決定する方法を提案し，従来手法以上の性能を持つことを実験的に示した．

３．多次元の実数データの集合の中から外れデータを検出することを目的に，多次元の実数値データにおける外れデータをLOO濃度に基づいて定義した上で，データ集合から構成されたBDDを用いて外れデータを高速に検出する方法を構成している．この手法も連続値と離散値の混在データに適用可能であり，従来手法と比較して，高精度かつ高速に外れデータを検出することを実験的に示している．

４．複数のECUがネットワークで繋がった車載システムの故障個所を特定することを目的に，モデルベース診断の枠組みに基づいてネットワークの機能を表現した論理式の最大充足可能性問題を解く際に，複雑なネットワーク内でのエラー信号の根源箇所を特定する方法を構成した．

これらの研究成果は，どれも全く新規な着想に基づいて行われている．車載システムの信頼性を向上させるという研究は主にソフトウェア工学の分野で研究されてきたが，本論文では，論理式を用いた抽象化と高速な論理演算の組み合わせを，ソフトウェア工学分野だけでなく機械学習分野において従来から研究されてきた枠組みに適用することで，新たな手法を構成しており，その独創性は特筆すべきである．また，提案している手法は既存のものと同等以上の性能を持つことを実験的に示しており，ソフトウェア工学分野と機械学習分野の双方に対する貢献度は高い．よって，本論文は博士（情報学）の学位論文として価値のあるものと認める．

また，平成２５年８月４日に実施した論文とそれに関連する内容についての口頭試問の結果，合格と認めた．

注)論文審査の結果の要旨の結句には、学位論文の審査についての認定を明記すること。
更に、試問の結果の要旨（例えば「平成　年　月　日論文内容とそれに関連した口頭試問を行った結果合格と認めた。」）を付け加えること。
Webでの即日公開を希望しない場合は、以下に公開可能とする日付を記入すること。
要旨公開可能日：　　年　　月　　日以降